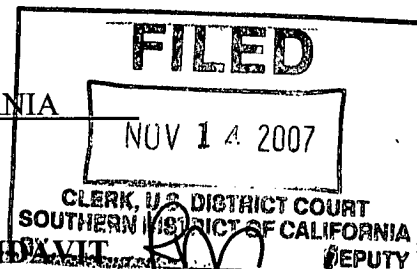


UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA



In the Matter of the Search of

Dell Dimension E521 desktop computer
Serial Number: HWC16C1

APPLICATION AND AFFIDAVIT

FOR SEARCH WARRANT

CASE NUMBER:

'07 MJ 2654

I, Jodi A. Jewett, being duly sworn depose and say:

I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that property or premises known as:

See Attachment A

in the Southern District of California there is now concealed a certain person or property, namely,

See Attachment B

which is: Subject to seizure under Rule 41(b)(1) of the Federal Rules of Criminal Procedure because the property constitutes evidence of the commission of criminal offenses or instrumentalities used in committing criminal offenses. The criminal offenses at issue are violations of: (1) Title 18, United States Code, Section 2251, production of child pornography as it relates to interstate or foreign commerce; (2) Title 18, United States Code, Section 2252A(a)(5)(B), possession of child pornography; (3) Title 18 United States Code Section 2252A(a)(2)(A), distribution receipt or distribution of child pornography, and Title 18, United States Code, Section 2252A(a)(2)(B), receipt or distribution of material containing child pornography.

The facts support a finding of Probable Cause are as follows:

See Affidavit of Jodi A. Jewett

Continued on the attached sheet and made a part thereof. ☒ Yes ☐ No

Jodi A. Jewett
Jodi A. Jewett
Special Agent
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence

11/9/07 at San Diego, California
Date City and State

CATHY ANN BENCIVENGO
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer

[Signature]
Signature of Judicial Officer

**AFFIDAVIT OF JODI JEWETT
IN SUPPORT OF SEARCH WARRANT**

I, Jodi A. Jewett, being duly sworn, do hereby depose and say:

BACKGROUND AND EXPERIENCE OF AFFIANT

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the Riverside resident agency in Riverside, California, and have been so employed since September 2006. I am assigned to a multi-agency child exploitation task force known as the Southern California Regional Sexual Assault Felony Enforcement Team ("SAFE Team"). As a SAFE Team member and an FBI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography. I am responsible for enforcing federal criminal statutes involving the sexual exploitation of children, and have conducted numerous investigations involving the possession, importation, and distribution of child pornography. I have completed approximately 136 hours of training in crimes against children, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography.

//

//

//

1 PURPOSE OF AFFIDAVIT

2 2. This affidavit is made in support of a search warrant
3 for four computers¹ seized during the execution of a search
4 warrant on July 24, 2007, for evidence of violations of Title 18,
5 United States Code, Section 2251, production of child pornography
6 as it relates to interstate or foreign commerce, Title 18, United
7 States Code, Section 2252A(a)(5)(B), possession of child
8 pornography, Title 18 United States Code, Section 2252A(a)(2)(A),
9 distribution receipt or distribution of child pornography, and
10 Title 18 United States Code, Section 2252A(a)(2)(B), receipt or
11 distribution of material containing child pornography.

12 3. The facts set forth in this affidavit are based upon my
13 personal observations, my training and experience, and
14 information obtained from other law enforcement officers and
15 witnesses. This affidavit is intended to show that there is
16 sufficient probable cause for the requested search warrant and
17 does not purport to set forth all of my knowledge of or
18 investigation into this matter.

19 THE ITEMS TO BE SEARCHED

20 4. The items to be searched consist of four computers
21 recovered by the California Department of Justice ("CAL-DOJ") on
22 July 24, 2007, from the residence of JAMES ALBERT SWEENEY II
23 ("SWEENEY") located at 4555 Mission Inn Avenue, Riverside,
24 California 92501. SWEENEY is currently under investigation for a
25 fraudulent scheme by CAL-DOJ.

26
27
28 ¹ The term "computer" as used in this affidavit, is
defined by 18 U.S.C. § 1030(e)(1).

1 5. The computers consist of the following:

2 a. Hewlett Packard M7000 desktop computer, bearing
3 serial number MXK60804L3;

4 b. Dell Dimension E521 desktop computer, bearing
5 serial number HWC16C1;

6 c. Hewlett Packard Touch Smart 1Q770 computer,
7 bearing serial number CNH7010011; and

8 d. Sony Vaio laptop computer, bearing serial number
9 VGINUX280P.

10 6. The four computers, as described above, are currently
11 in the custody of the Regional Computer Forensics Laboratory
12 ("RCFL") in San Diego, California. Additional computers were
13 also seized by CAL-DOJ investigators from SWEENEY's business and
14 storage facility, however, those computers are not a subject of
15 this search warrant.

16 THE ITEMS TO BE SEIZED

17 7. Based on the facts set forth in this affidavit, and my
18 experience investigating computer crimes as relates to crimes
19 against children, I submit that there is probable cause to
20 believe that the computers described above will contain evidence
21 of violations of: Title 18, United States Code, § 2251,
22 production of child pornography as it relates to interstate or
23 foreign commerce, Title 18, United States Code, § 2252A(a)(5)(B),
24 possession of child pornography, Title 18 United States Code, §
25 2252A(a)(2)(A), receipt or distribution of child pornography, and
26 Title 18 United States Code, § 2252A(a)(2)(B), receipt or
27 distribution of material containing child pornography.
28

1 8. More specifically, as described below, I believe that
2 there is probable cause that evidence of the following will be
3 found on the four computers as listed in ATTACHMENT A:

4 a. Files or records that tend to identify the
5 person(s) in control, possession, and ownership of the
6 computers identified in ATTACHMENT A or of any other
7 computers, including, but not limited to, canceled mail,
8 photographs, personal telephone books, diaries, bills and
9 statements, identification cards and documents, airline
10 tickets and related travel documents, bank books, checks,
11 and check registers, public storage facilities receipts,
12 computer registration records and sales receipts;

13 b. Images of child pornography, or materials
14 containing child pornography as defined in 18 U.S.C. Section
15 2256, which visually depict child pornography; contain
16 information pertaining to the interest in child pornography;
17 and/or distribute, receive, or possess child pornography, or
18 information pertaining to an interest in child pornography;

19 c. Files and records reflecting ownership, purchase,
20 possession, or use of computer devices or peripherals such
21 as web cameras and other video and audio recording devices,
22 that could be used to transmit live images over the Internet
23 or record images for later transmission over the Internet;

24 d. Files and records relating to the provision of
25 internet service, including billing and toll records;

26 e. Correspondence that are indicia of production,
27 possession, receipt, or distribution of child pornography
28 including, but not limited to, electronic mail, chat logs,

1 and electronic messages, establishing possession, access to,
2 receipt, production, distribution, or transmission through
3 interstate or foreign commerce, including by United States
4 mail or by computer, of visual depictions of minors engaged
5 in sexually explicit conduct, as defined in 18 U.S.C. §
6 2256;

7 f. Correspondence relating or referring to
8 exploitation of children including, but not limited to
9 electronic mail, chat logs, and electronic messages,
10 establishing possession, access to, or transmission through
11 interstate or foreign commerce of child pornography as
12 defined in 18 U.S.C. § 2256, including by United States mail
13 or by computer.

14 g. Files and records pertaining to possession,
15 production, receipt or distribution of child pornography, as
16 defined in 18 U.S.C. § 2256, including but not limited to:

17 (1) Envelopes, letters, and other correspondence
18 including, but not limited to, electronic mail, chat
19 logs, and electronic messages, establishing possession,
20 access to, or transmission through interstate or
21 foreign commerce, including by United States mail or by
22 computer, of visual depictions of minors engaged in
23 sexually explicit conduct, as defined in 18 U.S.C. §
24 2256; and

25 (2) Books, ledgers, and records bearing on the
26 production, reproduction, receipt, shipment, orders,
27 requests, trades, purchases, or transactions of any
28 kind involving the transmission through interstate or

1 foreign commerce including by United States mail or by
2 computer of any visual depiction of minors engaged in
3 sexually explicit conduct, as defined in 18 U.S.C. §
4 2256;

5 h. Any files or records relating to the exploitation
6 of minors.

7 i. Any files or records identifying individual e-mail
8 addresses and internet chat room names;

9 j. Any files or records showing the acquisition
10 and/or sale of computer hardware, computer software,
11 computer documentation, and/or computer passwords and other
12 data security devices;

13 k. Any files or records evidencing occupancy or
14 ownership of any residences and storage units registered to,
15 owned by, or controlled by JAMES ALBERT SWEENEY II,
16 including, but not limited to copies of utility and
17 telephone bills, mail envelopes, addressed correspondence
18 canceled mail, photographs, personal telephone books,
19 diaries, bills and statements, identification cards and
20 documents, airline tickets and related travel documents,
21 bank books, checks, and check registers, and public storage
22 facilities receipts.

23 l. Any files, records, programs, application or
24 materials, including but not limited to, images and
25 electronically stored computer data that would lead to the
26 identity of any minors as depicted in electronic images or
27 evidenced in electronic communications.
28

1 m. Mailing lists, mailing address labels and any and
2 all documents and records pertaining to any correspondence
3 between JAMES ALBERT SWEENEY II and any minor.

4 n. Any files or records related to ownership, control
5 and use of digital cameras, camcorders, or other recording
6 devices.

7 o. Electronic materials pertaining to the receipt of,
8 or orders or requests for visual depictions of a minor
9 involved in sexually explicit conduct, as defined in 18
10 U.S.C. § 2256;

11 p. Names, lists of names or addresses and identifying
12 information of minors (such as names and dates of birth of
13 minors).

14 q. As used above, the terms files, records, programs,
15 or correspondence includes files, records, programs, or
16 correspondence created, modified or stored in any form
17 including electronically.

18 TIMING OF SEARCH

19 9. As noted, the computers are currently in the possession
20 of RCFL. The computers will be searched by RCFL at the San Diego
21 facility upon authorization of this warrant. Consistent with the
22 requirements of Rule 41, the computers will be delivered to a
23 computer forensic technician at RCFL within 10 days of the
24 effective date of this warrant to commence the search. For the
25 reasons noted in paragraph 22 below, the search will not be
26 completed during the 10-day period. However, the computers will
27 be imaged, and will be preliminarily examined to determine
28 whether they contain any evidence or are an instrumentality of a

1 crime, within 60 days. If the computer forensic technicians
2 determine that the data does not fall within any of the items to
3 be seized pursuant to this warrant or is not otherwise legally
4 seized, the government will return these items within a
5 reasonable period of time not to exceed 60 days from the date of
6 execution of the warrant. If the government needs additional
7 time to determine whether the data falls within any of the items
8 to be seized pursuant to this warrant, it must obtain an
9 extension of the time period from the Court within the original
10 sixty day period.

11 INVESTIGATION

12 10. On or about October 2, 2007, I was contacted by
13 Riverside Police Department ("RPD") Detective James Dana and CAL-
14 DOJ Investigator Aaron L. Ward (Investigator Ward), who provided
15 me with the following information:

16 a. On July 24, 2007, CAL-DOJ executed a state search
17 warrant for evidence of fraud and grand theft, to include
18 any computer systems found, at SWEENEY's residence, storage
19 facility and business. Pursuant to the state fraud
20 investigation and execution of the state search warrants
21 attached hereto as ATTACHMENTS C and D, several of SWEENEY's
22 computer systems were seized. The items to be searched, as
23 described in ATTACHMENT A, were seized from SWEENEY's
24 residence.

25 b. Investigator Ward was a member of the law
26 enforcement team that searched SWEENEY's residence on July
27 24, 2007.
28

1 c. Prior to conducting the search, Investigator Ward
2 confirmed that SWEENEY owned the residence located at 4555
3 Mission Inn Avenue, Riverside California and that SWEENEY
4 was receiving mail at that residence. I further confirmed
5 with the United States Post Office, during the week of
6 October 8, 2007, that SWEENEY was the only person receiving
7 mail at that residence.

8 d. During the search of SWEENEY's residence,
9 Investigator Ward observed and later informed me of the
10 following:

11 (1) SWEENEY had two dogs on the premises, tan
12 colored dog that appeared to be a Golden Retriever and
13 a small dog that appeared to be a Chihuahua.

14 (2) The furniture in SWEENEY's residence was
15 ornate and rich looking.

16 (3) The bed in SWEENEY's master bedroom appeared
17 to be queen sized. The bed was framed in heavy, dark
18 wood.

19 (4) A Hewlett Packard M7000 desktop computer was
20 seized from SWEENEY's home office, upstairs across the
21 hallway from his master bedroom.

22 (5) Other computer systems, as described above,
23 were seized from SWEENEY's residence and storage
24 facility.

25 e. The Hewlett Packard M7000 desktop computer, along
26 with the other computers seized pursuant to the execution of
27 the search warrant were sent to RCFL in San Diego,
28 California for analysis by Investigator Ward.

1 f. On September 14, 2007, Investigator Ward spoke
2 with Riverside County Sheriff's Office Detective Peter Felt.
3 ("Detective Felt"). Detective Felt is a member of the
4 Riverside Computer and Technology Crime High-Technology
5 Response Team (C.A.T.C.H.). Detective Felt is currently
6 assigned to the RCFL in San Diego, California and was
7 responsible for imaging and analyzing the computers
8 submitted by Investigator Ward. Detective Felt told
9 Investigator Ward that in analyzing the Hewlett Packard
10 M7000 desktop computer seized from SWEENEY's home office,
11 Detective Felt discovered what appeared to be evidence of
12 child pornography.

13 11. Based upon my review of that state search warrants
14 executed by CAL-DOJ (see ATTACHMENTS C and D) I have learned the
15 following:

16 a. In his original affidavit, Investigator Ward
17 requested that "investigating officers, and those agents
18 acting under the direction of the investigating officer, be
19 authorized to access all computer data to determine if the
20 data contains property, records, and information"
21 (See page 17 of ATTACHMENT C). Investigator Ward further
22 explained that "the file name in the folder/directory is not
23 a reliable indicator of the true nature of its contents,
24 especially where there may be a desire on the user's part to
25 conceal certain records" (see page 14 of ATTACHMENT C).
26 Investigator Ward also provided that "computer users may
27 also conceal data through a number of methods, including the
28 use of misleading filenames and extensions. For example,

1 files with the extension .jpg are digital image files.
2 However, a computer user could change a .jpg file extension
3 to .txt or .dll, in order to create an appearance that a
4 digital image is actually a text or system file." (See page
5 14 of ATTACHMENT C)

6 b. Investigator Ward incorporated the original
7 affidavit, (ATTACHMENT C), into the supplemental affidavit,
8 (ATTACHMENT D), as indicated on page 2 of ATTACHMENT D.
9 Investigator Ward referred to the original affidavit as
10 exhibit 1. (See page 2 of ATTACHMENT D). Exhibit 1 refers
11 to the original affidavit and is now attached to this
12 document as ATTACHMENT C. Investigator Ward indicated that
13 "Records in the form of electronic files stored on computers
14 will be treated as indicated in Exhibit 1, pages 12-17."
15 (See page 6 of ATTACHMENT D).

16 c. Accordingly, after issuance of the search
17 warrants, Detective Felt conducted an initial preview of the
18 computer. While conducting this initial preview, Detective
19 Felt came upon an image, in plain view, that appeared to be
20 child pornography.

21 12. On November 8, 2007, Detective Felt advised me about
22 the specifics of conducting the computer analysis. Detective
23 Felt told me that to analyze the computer for evidence and
24 instrumentalities of the crimes alleged in the state search
25 warrant, Detective Felt did the following:

26 a. Detective Felt first made an image of the hard
27 drive of the Hewlett Packard M7000. Detective Felt then
28 used the Forensics Took Kit ("FTK") software in order to put

1 the data copied from the hard drive into separate
2 containers. Containers are the method of organization used
3 by FTK to separate computer data into workable sections.
4 Containers are assigned according to the information that is
5 put into them, and such containers include: graphics,
6 documents, email, explorer, search, and overview containers.
7 An item can be placed into more than one container, based
8 upon content. For example, a word document that contains an
9 image such as a business logo on it's letterhead, would be
10 placed into both the document and image containers.
11 Additionally a document could have been scanned and saved
12 into the computer, which would place it in the graphics
13 container, though it was originally a document. Therefore,
14 the names given to such containers can be misleading and it
15 should not be assumed that a document that contains evidence
16 of a crime could not reasonably be found in an image
17 container.

18 b. In conducting his initial preview and beginning
19 the forensic analysis of the Hewlett Packard M7000 imaged
20 hard drive, Detective Felt previewed each container that the
21 FTK software had generated. This is done both to ensure
22 that the FTK software functioned correctly and to attain an
23 initial look at potential evidence. Since any type of
24 document could reasonably be placed in any of the FTK
25 containers, depending upon how it was saved; all containers
26 are examined in a standard forensic analysis. When
27 Detective Felt looked in the graphics container for
28 documents and records pertaining to the fraud investigation,

1 he came upon an image, in plain view, that appeared to be
2 child pornography.

3 13. Investigator Ward further advised me on October 2, 2007
4 of the following:

5 a. On September 14, 2007, Detective Felt further told
6 Investigator Ward that Detective Felt discovered what
7 appeared to be one digital pornographic image and various
8 other digital images of young boys not fully dressed during
9 his analysis.

10 b. The pornographic image showed a picture of a young
11 boy, who appeared to be approximately twelve to fourteen
12 years of age. In this photograph, the boy is standing near
13 one side of a bed in what appears to be a bedroom at a
14 residence. The bed depicted in this image is framed in
15 heavy, dark wood. The young boy is wearing jeans and a blue
16 t-shirt. Two dogs, one dark colored and the other tan in
17 color, are also seen lying on the bed. The boy in the
18 picture is holding his erect penis in one hand while the
19 dark colored dog appears to be licking the boy's penis.

20 c. In a second digital photograph, an adult male is
21 seated on the opposite side of the same bed where the boy
22 was standing in the pornographic image described above in
23 paragraph 10(f)(3). The adult male is wearing a t-shirt and
24 underwear and is holding a laptop computer in his lap.
25 Investigator Ward further described the laptop as a Sony
26 Vaio. The two dogs from the pornographic image are also
27 seen in this picture.
28

1 d. In both pictures described in paragraphs 10(f)(3)
2 and 10(f)(4) above, the dogs appear to be lying in the same
3 place. In the picture featuring the adult male, the dogs
4 are on the left side of the bed near the adult male's feet.
5 In the pornographic picture, the dogs are on the left side
6 of the bed in the same position as in the picture featuring
7 the adult male. Detective Felt also noted that the bed, the
8 bedspread, and the lighting appeared to be the same in both
9 pictures. Detective Felt stated that the camera angle
10 changed between the two photographs and the different angles
11 would have allowed for both the adult male and the twelve to
12 fourteen year old boy to be in the same location at the same
13 time and be featured in two different photographs.

14 e. Based on his training and experience, Detective
15 Felt believed that these two photographs were taken at
16 approximately the same time and at the same location.

17 14. On September 18, 2007 Investigator Ward met with
18 Detective Felt at the RCFL in San Diego, California. The images
19 described above were shown to Investigator Ward. After this
20 meeting, Investigator Ward told me that he recognized the bed in
21 the two photographs as being the bed that Investigator Ward saw
22 at SWEENEY's residence during the execution of the search warrant
23 at 4555 Mission Inn Avenue in Riverside California on July 24,
24 2007.² Investigator Ward looked at the second photograph

25
26 ² Although investigators did not see the dark colored dog
27 depicted in the pornographic image when at SWEENEY's residence
28 during execution of the search warrant on July 24, 2007, it is
 unclear whether the tan colored dog was one of the two dogs seen
 at SWEENEY's residence during execution of the search warrant.

1 involving the adult male as described in paragraph 10(f)(4) above
2 and told me that he recognized the adult male seated on the bed
3 as SWEENEY.³ Investigator Ward made the identification of
4 SWEENEY based on looking at photographs of SWEENEY and from
5 personally meeting SWEENEY on August 21, 2007.

6 15. I subsequently learned that SWEENEY was the registered
7 owner of the residence located at 4555 Mission Inn Avenue
8 Riverside CA 92501 by conducting a query of the ACCURINT
9 database. The query revealed that the residence was registered to
10 James A. SWEENEY II. I then confirmed SWEENEY's name as it
11 appears on his California driver's license, number DXXXX259, as
12 James Albert Sweeney II.

13 16. I also learned that SWEENEY owns a second residence in
14 Afton, Tennessee. A query of the ACCUPRINT database for this
15 residence in Tennessee also revealed that James A. Sweeney II was
16 the registered owner of that residence.

17 17. On October 3, 2007, I learned that at some time after
18 execution of the CAL-DOJ search warrant on July 24, 2007,
19 SWEENEY's attorney advised CAL-DOJ investigators that SWEENEY was
20 currently staying at the residence in Tennessee.

21 18. I also learned thereafter that Detective Felt relayed
22 the following information to Investigator Ward:
23
24

25 ³ The computer depicted in the photo of SWEENEY seated on
26 the bed has not been seized by law enforcement authorities and
27 its location is currently unknown. The Sony Vaio currently in
28 the possession of RCFL is a small sized Sony Vaio where as the
Sony Vaio laptop depicted in the image as described in paragraph
10(f)(4) above is a full size laptop.

1 a. During his initial preview of the Hewlett Packard
2 M7000 desktop computer, Detective Felt also viewed a number
3 of other images of young boys in various stages of undress.

4 b. One of these images was a photograph of a young
5 boy, approximately ten years old, in a bathtub. The boy
6 seated in the bathtub can only be seen from the waist up.

7 c. Similarly, in many of the other photographs, the
8 boys were shirtless with their pants pulled low, but not
9 exposing their pubic area.

10 d. Detective Felt also retrieved five images from the
11 Hewlett Packard M7000 desktop computer for purposes of
12 identifying the individuals depicted in these images.
13 Detective Felt chose the five images to include the faces of
14 four boys he had seen most frequently during his preview of
15 the Hewlett Packard M7000 computer, including the face of
16 the boy seen in the child pornography image described in
17 paragraph 10(f)(3) above.

18 e. Within these five preliminary images, Detective
19 Felt included one image that included the adult male seen on
20 the bed as described in paragraph 10(f)(4) above. These
21 preliminary images, hereinafter referred to as "Preliminary
22 Images" 1, 2, 3, 4, and 5 are further described below:

23 (1) Preliminary Image 1 depicts a teenaged boy
24 with dirty blond hair, brown or hazel eyes, and a
25 grimace on his face. The boy is wearing a grey t-shirt
26 and a white beaded necklace with three red beads spaced
27 within the white beads of the necklace. The individual
28 depicted in Preliminary Image 1 is the same individual

1 depicted in the child pornography image as described in
2 paragraph 10(f)(3) above.

3 (2) Preliminary Image 2 depicts a young boy with
4 shaggy blond hair and brown or hazel eyes. The boy is
5 wearing blue jeans and a grey t-shirt with the word
6 "etnies" in white letters on the front of the t-shirt.
7 The boy is standing with his right hand behind his head
8 and his left hand pulled to the left underarm. The boy
9 is wearing what appears to be black wrist braces on
10 both wrists.

11 (3) Preliminary Image 3 depicts a young boy with
12 short, dirty blond hair and brown or hazel eyes. The
13 boy is wearing a black t-shirt with a red thorn-like
14 line across the chest. The boy is displaying the peace
15 sign with his left hand.

16 (4) Preliminary Image 4 depicts a young boy with
17 blond hair and blue eyes. The boy is wearing a green
18 sweatshirt with the word "quicksilver" in white letters
19 across the front of the sweatshirt. The boy is
20 standing or sitting near a red leather chair and a
21 statue can be seen behind him.

22 (5) Preliminary Image 5 depicts the same teenaged
23 boy as in Preliminary Image 1. In this image, the boy
24 is wearing a blue t-shirt and what appears to be the
25 same white necklace. The boy is standing behind and to
26 the left of an adult male. The adult male is SWEENEY.
27 SWEENEY is wearing a yellow sweatshirt and a baseball
28 cap with an unknown symbol on the front.

1 19. On October 2, 2007, a conference call was conducted
2 between myself, Investigator Ward, and Detective Dana, where I
3 learned the following:

4 a. Investigator Ward positively identified the
5 location at which the pornographic photograph described in
6 paragraph 10(f)(3) above was taken. Investigator Ward
7 stated that when the search of SWEENEY's residence was
8 conducted on July 24, 2007, Investigator Ward was in the
9 residence and recalled seeing the bed in SWEENEY's bedroom
10 as seen in both the pornographic image and the image of
11 SWEENEY sitting on the bed.

12 b. Investigator Ward further advised that when he
13 viewed the photograph depicting SWEENEY sitting on the bed,
14 he believed that the photograph had been taken recently.
15 Investigator Ward stated that SWEENEY, whom he identified as
16 the adult male on the bed, looked the same in that
17 photograph as he did when he met with SWEENEY on August 21,
18 2007. Investigator Ward further stated that the furniture,
19 specifically the bed, looked to be the same as the furniture
20 that Investigator Ward encountered during the execution of
21 the search warrant.

22 20. Further investigation into this matter was conducted by
23 myself and Detective Dana. On October 2, 2007, Detective Dana
24 and I went to SWEENEY's residence located at 4555 Mission Inn
25 Avenue, in Riverside California and observed the following:

26 a. From our observation through the front window of
27 the residence, the residence appeared to be occupied and the
28 lights including the television were on;

1 b. Detective Dana and I approached the front door of
2 the residence and observed a small child sized bicycle
3 laying on its side in the front hallway near the stairway.
4 A stuffed animal was also seen placed on a window sill.

5 c. A white Chevrolet pickup truck was parked in the
6 back driveway of the residence bearing California license
7 plate number 7R75106. A query of this license plate
8 returned a result for an Ernest L. Werkheiser of Milditas,
9 California.

10 21. Detective Dana then obtained RPD Report P07-072881
11 regarding a police contact on May 13, 2007 at SWEENEY's residence
12 located at 4555 Mission Inn Avenue, Riverside, California. The
13 report provided the following:

14 a. RPD Officer J. Mattson responded to a drunk in
15 public call located at the residence. Upon arrival, SWEENEY
16 told Officer Mattson that he was a family friend of the
17 Williams family. SWEENEY told the officer that Kenneth Dale
18 Williams ("Mr. Williams") is a homeless father with four
19 sons, and Mr. Williams drops off his sons at SWEENEY's
20 residence every morning for purposes of preparing for
21 school.

22 b. On May 13, 2007, Mr. Williams left one of his
23 sons, age fourteen, with SWEENEY. When Mr. Williams came
24 back to SWEENEY's residence to pick up his son, SWEENEY
25 thought that Mr. Williams was under the influence and called
26 the RPD.

27 c. Mr. Williams' son told Officer Mattson that his
28 father, Mr. Williams, beat him and his brothers. Officer

1 Mattson visually examined the child but was unable to locate
2 any signs of physical abuse.

3 22. On October 4, 2007, Preliminary Images 1 - 5 as
4 described in paragraphs 14(e) (1-5), were taken to the "Circle of
5 Life" homeless shelter where Mr. Williams and his four sons had
6 been residing for the past three years. Carrie Walker ("Ms.
7 Walker"), is a staff member at the shelter and provided the
8 following information:

9 a. Ms. Walker has known the Williams family for the
10 past three years. Ms. Walker positively identified all the
11 individuals depicted in Preliminary Images 1 - 5.

12 b. Ms. Walker identified the four young boys depicted
13 in Preliminary Images 1 - 5 as Mr. Williams' sons.

14 c. Ms. Walker also identified the adult male depicted
15 in Preliminary Image 5 as the man that the children referred
16 to as "Uncle Jimmy." Ms. Walker further stated that the
17 boys spoke fondly of "Uncle Jimmy" and they told Ms. Walker
18 that Uncle Jimmy bought them expensive toys and video games.

19 d. Ms. Walker further stated that she last saw the
20 Williams family approximately one month ago wherein they
21 told Ms. Walker that they were moving in with a family in
22 Arkansas.

23 e. Ms. Walker advised that Mr. Williams had stopped
24 allowing his sons to go to "Uncle Jimmy's" residence, but
25 never stated why. Mr. Williams told Ms. Walker that he was
26 getting his life back together and it was time to take care
27 of his sons.
28

1 f. Ms. Walker stated that she met "Uncle Jimmy" once,
2 approximately three weeks prior to October 4, 2007 when
3 "Uncle Jimmy" came to the shelter looking for the Williams
4 family.

5 g. Ms. Walker provided copies of the Social Security
6 Cards for Mr. Williams and all four of his sons. She also
7 provided a photograph of Mr. Williams and a copy of his
8 California Driver's License.

9 23. After researching various databases by using the social
10 security numbers provided by Ms. Walker, I was able to determine
11 that the four boys depicted in Preliminary Images 1 -5 currently
12 range from ages ten to sixteen years old.

13 USE OF CAMERAS AND COMPUTERS

14 24. Based upon my own knowledge, training, and experience
15 in child exploitation and child pornography investigations, and
16 the experience and training of other law enforcement officers
17 with whom I have had discussions, I am aware of the following
18 regarding the use of computers and cameras relating to child
19 pornography and child exploitation:

20 a. The development of computers has revolutionized
21 the way in which those who seek out child pornography are
22 able to obtain this material. Computers serve four basic
23 functions in connection with child pornography: production,
24 communication, distribution, and storage.

25 b. Producers of child pornography can now produce
26 both still and moving images directly from a common video or
27 digital camera. The camera is attached, using a device such
28 as a cable, or digital images are often uploaded from the

1 camera's memory card, directly to the computer. Images can
2 then be stored, manipulated, transferred, or printed
3 directly from the computer. As a result of this technology,
4 it is relatively inexpensive and technically easy to
5 produce, store, and distribute child pornography.

6 c. The Internet allows users, while still maintaining
7 anonymity, to easily locate (i) other individuals with
8 similar interests in child pornography; and (ii) websites
9 that offer images of child pornography. Those who seek to
10 obtain images or videos of child pornography can use
11 standard Internet connections, such as those provided by
12 businesses, universities, and government agencies, to
13 communicate with each other and to distribute or receive
14 child pornography. These communication links allow contacts
15 around the world as easily as calling next door.
16 Additionally, these communications can be quick, relatively
17 secure, and as anonymous as desired. All of these
18 advantages, which promote anonymity for both the distributor
19 and recipient, are well known and are the foundation of
20 transactions involving those who wish to gain access to
21 child pornography over the Internet. Sometimes, the only
22 way to identify both parties and verify the transportation
23 of child pornography over the Internet is to examine the
24 recipient's computer, in order to look for "footprints" of
25 the websites and images accessed by the recipient.

26 d. The computer's capability to store images in
27 digital form makes it an ideal repository for child
28 pornography. A single floppy or compact disk can store

1 dozens of images and hundreds of pages of text. The size of
2 the electronic storage media used in home computers
3 (commonly referred to as a hard drive) has grown
4 tremendously within the last several years. Hard drives
5 with the capacity of 40 gigabytes are not uncommon. These
6 drives can store thousands of images at very high
7 resolution. Moreover, electronic files downloaded to a hard
8 drive can be stored for years at little to no cost.

9 e. Computer files or remnants of such files can be
10 recovered months or even years after they have been
11 downloaded onto a hard drive, deleted, or viewed via the
12 Internet. Even when such files have been deleted, they can
13 be recovered months or years later using readily-available
14 forensic tools. When a person "deletes" a file on a home
15 computer, the data contained in the file does not actually
16 disappear; rather, that data remains on the hard drive until
17 it is overwritten by new data. Therefore, deleted files, or
18 remnants of deleted files, may reside in free space or slack
19 space - that is, in space on the hard drive that is not
20 allocated to an active file or that is unused after a file
21 has been allocated to a set block of storage space - for
22 long periods of time before they are overwritten. In
23 addition, a computer's operating system may also keep a
24 record of deleted data in a "swap" or "recovery" file.
25 Similarly, files that have been viewed via the Internet are
26 automatically downloaded into a temporary Internet directory
27 or cache. The browser typically maintains a fixed amount of
28 hard drive space devoted to these files, and the files are

1 only overwritten as they are replaced with more recently
2 viewed Internet pages. Thus, the ability to retrieve
3 residue of an electronic file from a hard drive depends less
4 on when the file was downloaded or viewed, than on a
5 particular user's operating system, storage capacity, and
6 computer habits.

7 f. Individuals who commit crimes against children via
8 computers do not readily discard the computer, as computers
9 are expensive items that are typically used for years before
10 being upgraded or discarded.

11 g. Individuals who commit these types of crimes often
12 keep electronic records of activities on their computers.
13 This information often includes logs of fraudulent
14 transaction history, monies received, individuals that have
15 been victimized, and payments to or from co-conspirators.

16 h. Individuals who possess child pornography often
17 store evidence of child pornography on multiple computer
18 systems and storage devices.

19 i. The memory cards in digital cameras have the
20 capacity to store hundreds, if not thousands, of digital
21 photographs.

22 j. Individuals who utilize digital cameras upload
23 their digital photos from the memory cards of digital
24 cameras to their computers, zip drives or other electronic
25 storage devices for viewing, printing and storing.

26 k. Individuals who possess images of child
27 pornography tend to trade or distribute their images on the
28

1 internet for the purpose of receiving additional child
2 pornography images.

3 25. Based on the foregoing, I believe additional evidence
4 of violations of Title 18, United States Code, Section 2251,
5 production of child pornography as it relates to interstate or
6 foreign commerce, Title 18, United States Code, Section
7 2252A(a)(5)(B), possession of child pornography, Title 18 United
8 States Code, Section 2252A(a)(2)(A), distribution receipt or
9 distribution of child pornography, and Title 18 United States
10 Code, Section 2252A(a)(2)(B), receipt or distribution of material
11 containing child pornography exists on the other computer systems
12 that were seized from SWEENEY's residence.

13 COMPUTER DATA

14 26. Based upon my training, experience and information
15 related to me by agents and others involved in the forensic
16 examination of computers, I know that computer data can be stored
17 on a variety of systems and storage devices including hard disk
18 drives, floppy disks, compact disks, magnetic tapes and memory
19 chips. I also know that during the search of the premises it is
20 not always possible to search computer equipment and storage
21 devices for data for a number of reasons, including the
22 following:

23 a. Searching computer systems is a highly technical
24 process which requires specific expertise and specialized
25 equipment. There are so many types of computer hardware and
26 software in use today that it is impossible to bring to the
27 search site all of the necessary technical manuals and
28 specialized equipment necessary to conduct a thorough

1 search. In addition, it may also be necessary to consult
2 with computer personnel who have specific expertise in the
3 type of computer, software application or operating system
4 that is being searched.

5 b. Searching computer systems requires the use of
6 precise, scientific procedures which are designed to
7 maintain the integrity of the evidence and to recover
8 "hidden," erased, compressed, encrypted or password-
9 protected data. Computer hardware and storage devices may
10 contain "booby traps" that destroy or alter data if certain
11 procedures are not scrupulously followed. Since computer
12 data is particularly vulnerable to inadvertent or
13 intentional modification or destruction, a controlled
14 environment, such as a law enforcement laboratory, is
15 essential to conducting a complete and accurate analysis of
16 the equipment and storage devices from which the data will
17 be extracted.

18 c. The volume of data stored on many computer systems
19 and storage devices will typically be so large that it will
20 be highly impractical to search for data during the
21 execution of the physical search of the premises. A single
22 megabyte of storage space is the equivalent of 500 double-
23 spaced pages of text. A single gigabyte of storage space,
24 or 1,000 megabytes, is the equivalent of 500,000 double-
25 spaced pages of text. Storage devices capable of storing
26 fifteen gigabytes of data are now commonplace in desktop
27 computers. Consequently, each non-networked, desktop
28 computer found during a search can easily contain the

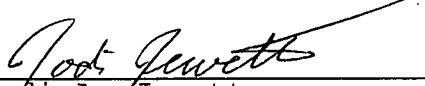
1 equivalent of 7.5 million pages of data, which, if printed
2 out, would completely fill a 10' x 12' x 10' room to the
3 ceiling.

4 d. Computer users can attempt to conceal data within
5 computer equipment and storage devices through a number of
6 methods, including the use of innocuous or misleading
7 filenames and extensions. For example, files with the
8 extension ".jpg" often are image files; however, a user can
9 easily change the extension to ".txt" to conceal the image
10 and make it appear that the file contains text. Computer
11 users can also attempt to conceal data by using encryption,
12 which means that a password or device, such as a "dongle" or
13 "keycard," is necessary to decrypt the data into readable
14 form. In addition, computer users can conceal data within
15 another seemingly unrelated and innocuous file in a process
16 called "steganography." For example, by using steganography
17 a computer user can conceal text in an image file which
18 cannot be viewed when the image file is opened. Therefore,
19 a substantial amount of time is necessary to extract and
20 sort through data that is concealed or encrypted to
21 determine whether it is evidence, contraband or
22 instrumentalities of a crime.

23 CONCLUSION:

24 27. Based upon the foregoing, I believe that there is
25 probable cause to believe that the (1) Hewlett Packard M7000
26 desktop computer, bearing serial number MXK60804L3, (2) a Dell
27 Dimension E521 desktop computer, bearing serial number HWC16C1,
28 (3) a Hewlett Packard Touch Smart 1Q770 computer, bearing serial

1 number CNH7010011, and (4) a Sony Vaio laptop computer, bearing
2 serial number VGUNIX280P, contain evidence of violations of Title
3 18, United States Code, Section 2251, production of child
4 pornography as it relates to interstate or foreign commerce,
5 Title 18, United States Code, Section 2252A(a) (5) (B), possession
6 of child pornography, Title 18 United States Code, Section
7 2252A(a) (2) (A), distribution receipt or distribution of child
8 pornography, and Title 18 United States Code, Section
9 2252A(a) (2) (B), receipt or distribution of material containing
10 child pornography.

11
12
13 
14 Jodi A. Jewett
Special Agent
Federal Bureau of Investigation

15 Subscribed and sworn to before me
16 this 9th day of November, 2007

17
18 
19 UNITED STATES MAGISTRATE JUDGE
20 **CATHY ANN BENCIVENGO**

ATTACHMENT A

ITEMS TO BE SEARCHED

The ITEMS TO BE SEARCHED are further described as follows:

- a. Hewlett Packard M7000 desktop computer serial number MXK60804L3 and all hardware and software attached to, or otherwise accompanying this computer as seized;
- b. Dell Dimension E521 desktop computer serial number HWC16C1 and all hardware and software attached to, or otherwise accompanying this computer as seized;
- c. Hewlett Packard Touch Smart 1Q770 computer serial number CNH7010011 and all hardware and software attached to, or otherwise accompanying this computer as seized;
- d. Sony Vaio laptop computer serial number VGUNIX280P and all hardware and software attached to, or otherwise accompanying this computer as seized;

ATTACHMENT B

ITEMS TO BE SEIZED

1. The following are the ITEMS TO BE SEIZED from the ITEMS TO BE SEARCHED, which constitute evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 2251, production of child pornography as it relates to interstate or foreign commerce, Title 18, United States Code, Section 2252A(a)(5)(B), possession of child pornography, Title 18 United States Code, Section 2252A(a)(2)(A), distribution receipt or distribution of child pornography, and Title 18 United States Code, Section 2252A(a)(2)(B), receipt or distribution of material containing child pornography:

a. Files or records that tend to identify the person(s) in control, possession, and ownership of the computers identified in ATTACHMENT A or of any other computers, including, but not limited to, canceled mail, photographs, personal telephone books, diaries, bills and statements, identification cards and documents, airline tickets and related travel documents, bank books, checks, and check registers, public storage facilities receipts, computer registration records and sales receipts;

b. Images of child pornography, or materials containing child pornography as defined in 18 U.S.C. Section 2256, which visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography;

1 c. Files and records reflecting ownership, purchase,
2 possession, or use of computer devices or peripherals such
3 as web cameras and other video and audio recording devices,
4 that could be used to transmit live images over the Internet
5 or record images for later transmission over the Internet;

6 d. Files and records relating to the provision of
7 internet service, including billing and toll records;

8 e. Correspondence that are indicia of production,
9 possession, receipt, or distribution of child pornography
10 including, but not limited to, electronic mail, chat logs,
11 and electronic messages, establishing possession, access to,
12 receipt, production, distribution, or transmission through
13 interstate or foreign commerce, including by United States
14 mail or by computer, of visual depictions of minors engaged
15 in sexually explicit conduct, as defined in 18 U.S.C. §
16 2256;

17 f. Correspondence relating or referring to
18 exploitation of children including, but not limited to
19 electronic mail, chat logs, and electronic messages,
20 establishing possession, access to, or transmission through
21 interstate or foreign commerce of child pornography as
22 defined in 18 U.S.C. § 2256, including by United States mail
23 or by computer.

24 g. Files and records pertaining to possession,
25 production, receipt or distribution of child pornography, as
26 defined in 18 U.S.C. § 2256, including but not limited to:

27 (1) Envelopes, letters, and other correspondence
28 including, but not limited to, electronic mail, chat

1 logs, and electronic messages, establishing possession,
2 access to, or transmission through interstate or
3 foreign commerce, including by United States mail or by
4 computer, of visual depictions of minors engaged in
5 sexually explicit conduct, as defined in 18 U.S.C. §
6 2256; and

7 (2) Books, ledgers, and records bearing on the
8 production, reproduction, receipt, shipment, orders,
9 requests, trades, purchases, or transactions of any
10 kind involving the transmission through interstate or
11 foreign commerce including by United States mail or by
12 computer of any visual depiction of minors engaged in
13 sexually explicit conduct, as defined in 18 U.S.C. §
14 2256;

15 h. Any files or records relating to the exploitation
16 of minors.

17 i. Any files or records identifying individual e-mail
18 addresses and internet chat room names;

19 j. Any files or records showing the acquisition
20 and/or sale of computer hardware, computer software,
21 computer documentation, and/or computer passwords and other
22 data security devices;

23 k. Any files or records evidencing occupancy or
24 ownership of any residences and storage units registered to,
25 owned by, or controlled by JAMES ALBERT SWEENEY II,
26 including, but not limited to copies of utility and
27 telephone bills, mail envelopes, addressed correspondence
28 canceled mail, photographs, personal telephone books,

1 diaries, bills and statements, identification cards and
2 documents, airline tickets and related travel documents,
3 bank books, checks, and check registers, and public storage
4 facilities receipts.

5 l. Any files, records, programs, application or
6 materials, including but not limited to, images and
7 electronically stored computer data that would lead to the
8 identity of any minors as depicted in electronic images or
9 evidenced in electronic communications.

10 m. Mailing lists, mailing address labels and any and
11 all documents and records pertaining to any correspondence
12 between JAMES ALBERT SWEENEY II and any minor.

13 n. Any files or records related to ownership, control
14 and use of digital cameras, camcorders, or other recording
15 devices.

16 o. Electronic materials pertaining to the receipt of,
17 or orders or requests for visual depictions of a minor
18 involved in sexually explicit conduct, as defined in 18
19 U.S.C. § 2256;

20 p. Names, lists of names or addresses and identifying
21 information of minors (such as names and dates of birth of
22 minors).

23 q. As used above, the terms files, records, programs,
24 or correspondence includes files, records, programs, or
25 correspondence created, modified or stored in any form
26 including electronically.

ATTACHMENT A

ITEMS TO BE SEARCHED

The ITEMS TO BE SEARCHED are further described as follows:

- a. Hewlett Packard M7000 desktop computer serial number MXK60804L3 and all hardware and software attached to, or otherwise accompanying this computer as seized;
- b. Dell Dimension E521 desktop computer serial number HWC16C1 and all hardware and software attached to, or otherwise accompanying this computer as seized;
- c. Hewlett Packard Touch Smart 1Q770 computer serial number CNH7010011 and all hardware and software attached to, or otherwise accompanying this computer as seized;
- d. Sony Vaio laptop computer serial number VGUNIX280P and all hardware and software attached to, or otherwise accompanying this computer as seized;

ATTACHMENT B

ITEMS TO BE SEIZED

1. The following are the ITEMS TO BE SEIZED from the ITEMS TO BE SEARCHED, which constitute evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 2251, production of child pornography as it relates to interstate or foreign commerce, Title 18, United States Code, Section 2252A(a)(5)(B), possession of child pornography, Title 18 United States Code, Section 2252A(a)(2)(A), distribution receipt or distribution of child pornography, and Title 18 United States Code, Section 2252A(a)(2)(B), receipt or distribution of material containing child pornography:

a. Files or records that tend to identify the person(s) in control, possession, and ownership of the computers identified in ATTACHMENT A or of any other computers, including, but not limited to, canceled mail, photographs, personal telephone books, diaries, bills and statements, identification cards and documents, airline tickets and related travel documents, bank books, checks, and check registers, public storage facilities receipts, computer registration records and sales receipts;

b. Images of child pornography, or materials containing child pornography as defined in 18 U.S.C. Section 2256, which visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography;

1 c. Files and records reflecting ownership, purchase,
2 possession, or use of computer devices or peripherals such
3 as web cameras and other video and audio recording devices,
4 that could be used to transmit live images over the Internet
5 or record images for later transmission over the Internet;

6 d. Files and records relating to the provision of
7 internet service, including billing and toll records;

8 e. Correspondence that are indicia of production,
9 possession, receipt, or distribution of child pornography
10 including, but not limited to, electronic mail, chat logs,
11 and electronic messages, establishing possession, access to,
12 receipt, production, distribution, or transmission through
13 interstate or foreign commerce, including by United States
14 mail or by computer, of visual depictions of minors engaged
15 in sexually explicit conduct, as defined in 18 U.S.C. §
16 2256;

17 f. Correspondence relating or referring to
18 exploitation of children including, but not limited to
19 electronic mail, chat logs, and electronic messages,
20 establishing possession, access to, or transmission through
21 interstate or foreign commerce of child pornography as
22 defined in 18 U.S.C. § 2256, including by United States mail
23 or by computer.

24 g. Files and records pertaining to possession,
25 production, receipt or distribution of child pornography, as
26 defined in 18 U.S.C. § 2256, including but not limited to:

27 (1) Envelopes, letters, and other correspondence
28 including, but not limited to, electronic mail, chat

1 logs, and electronic messages, establishing possession,
2 access to, or transmission through interstate or
3 foreign commerce, including by United States mail or by
4 computer, of visual depictions of minors engaged in
5 sexually explicit conduct, as defined in 18 U.S.C. §
6 2256; and

7 (2) Books, ledgers, and records bearing on the
8 production, reproduction, receipt, shipment, orders,
9 requests, trades, purchases, or transactions of any
10 kind involving the transmission through interstate or
11 foreign commerce including by United States mail or by
12 computer of any visual depiction of minors engaged in
13 sexually explicit conduct, as defined in 18 U.S.C. §
14 2256;

15 h. Any files or records relating to the exploitation
16 of minors.

17 i. Any files or records identifying individual e-mail
18 addresses and internet chat room names;

19 j. Any files or records showing the acquisition
20 and/or sale of computer hardware, computer software,
21 computer documentation, and/or computer passwords and other
22 data security devices;

23 k. Any files or records evidencing occupancy or
24 ownership of any residences and storage units registered to,
25 owned by, or controlled by JAMES ALBERT SWEENEY II,
26 including, but not limited to copies of utility and
27 telephone bills, mail envelopes, addressed correspondence
28 canceled mail, photographs, personal telephone books,

1 diaries, bills and statements, identification cards and
2 documents, airline tickets and related travel documents,
3 bank books, checks, and check registers, and public storage
4 facilities receipts.

5 l. Any files, records, programs, application or
6 materials, including but not limited to, images and
7 electronically stored computer data that would lead to the
8 identity of any minors as depicted in electronic images or
9 evidenced in electronic communications.

10 m. Mailing lists, mailing address labels and any and
11 all documents and records pertaining to any correspondence
12 between JAMES ALBERT SWEENEY II and any minor.

13 n. Any files or records related to ownership, control
14 and use of digital cameras, camcorders, or other recording
15 devices.

16 o. Electronic materials pertaining to the receipt of,
17 or orders or requests for visual depictions of a minor
18 involved in sexually explicit conduct, as defined in 18
19 U.S.C. § 2256;

20 p. Names, lists of names or addresses and identifying
21 information of minors (such as names and dates of birth of
22 minors).

23 q. As used above, the terms files, records, programs,
24 or correspondence includes files, records, programs, or
25 correspondence created, modified or stored in any form
26 including electronically.

ATTACHMENT C

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

07180701

06270702

2007 JUN 27 AM 9:27

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

EXPERIENCE AND TRAINING OF AFFIANT

2

3 I, Aaron L. Ward, am an Investigator with the California Department of Justice (DOJ),
4 Special Crimes Unit, Office of the Attorney General. I have been employed as an Investigator with
5 the Department of Justice since April 2, 2001. Prior to my employment as an investigator with the
6 California Department of Justice, I was an United States Postal Inspector assigned to the Southern
7 California Division of the United States Postal Inspection Service. I retired from the position of
8 Postal Inspector on March 30, 2001, and took my current position. I was a Postal Inspector for
9 twenty years. For the last ten years of my Inspection Service career, my responsibilities included
10 investigating crimes involving mail fraud and supervising the activities of five other Postal
11 Inspectors. I have extensive experience investigating crimes involving financial transactions,
12 investment fraud schemes (including Ponzi schemes), and money laundering.

13 I completed an eleven week training course for Postal Inspectors at the United States Postal
14 Inspection Service (USPIS) Academy at Potomac, MD. I have attended both basic and complex
15 fraud training courses at the USPIS Academy in Potomac, MD. Additionally, I have received money
16 laundering and asset forfeiture training at the USPIS Academy in Potomac, MD. I have received
17 bankruptcy fraud training at the United States Attorney's Office (USAO), Central District of
18 California (CDC), Los Angeles, CA.

19 I have provided training on workers' compensation fraud investigations to other postal
20 inspectors. I have testified as an expert witness for the USAO, CDC, Los Angeles, CA.. related to
21 telemarketing fraud investigations.

22 I have been a participant in the United States Attorney's Office, Southern California,
23 Investment Fraud Task Force, formed to pool resources and experiences in the investigation of
24 violations and abuses in the area of "boiler room" schemes. I have also been a member of the
25 County of Orange Boiler room Apprehension (COBRA) Task Force, which was comprised of
26 various federal and state agencies that investigated alleged telemarketing "boiler room" fraud.

27 During my career as a postal inspector, I have been the affiant on approximately 60 search
28 warrant affidavits, requesting to search and seize electronic files contained in computer equipment.

06270702

1 bank accounts, brokerage accounts, and records from business and residential premises. In virtually
2 every instance in which a search warrant was issued, I found evidence of the crime alleged. I am
3 familiar with the United States Code and the California Penal Code relating to financial crimes,
4 conspiracy, and the rules of evidence.

5 INTRODUCTION

6 This case was referred to the Department of Justice, Office of the Attorney General, in April
7 2007, after complaints by investors about the individuals and companies discussed below. The
8 Department of Justice enforcement attorney, Kirk Wallace, referred the case for the reason that it
9 was believed the below described individuals were operating an endless chain marketing scheme
10 and had defrauded investors of approximately \$5 Million in unregistered stock, in addition to selling
11 memberships, in violation of the California Corporate Securities laws, as well as the California Penal
12 Code.

13 MISREPRESENTATIONS/OMISSIONS

14 On June 20, 2007, I reviewed a Desist and Refrain order against James Albert Sweeney, II,
15 Richard Hickey, Patrick Ryan, and Rick Deluca doing business as Big Co op, Inc. and EZ2Win.Biz,
16 Inc. The Desist and Refrain (D and R) order was issued because James Albert Sweeney, II, Richard
17 Hickey, Patrick Ryan, and Rick Deluca doing business as Big Co op, Inc. and EZ2Win.Biz were
18 offering unregistered and unlicensed securities to the public. The D and R order pointed out that
19 James Albert Sweeney, II, Richard Hickey, Patrick Ryan, and Rick Deluca doing business as Big
20 Co op, Inc. and EZ2Win.Biz, Inc. failed to advise their investors of the following:

- 21 1. That the public offering of Big Co op, Inc. stock still had not occurred several years
22 after prior purchasers had been told it would occur.
- 23 2. That Big Co op, Inc. had made no significant effort to prepare the required
24 documents such as audited financial statements or business plans which would be
25 required to take the company public and had not applied to any State or Federal
26 regulatory agencies to be permitted to offer publicly traded stock.
- 27 3. That the statements made to license purchasers in 2006 that Thomas Wiesel Partners
28 was going to take Big Co op, Inc. public in December of 2006 was also untrue in that

06270702

1 no request had been made at that time by Big Co op, Inc. to Thomas Wiesel Partners
2 to take any action or make any preparations to take Big Co op, Inc. public in
3 December of 2006, or at any other time.

- 4 4. That purchasers of licenses were not told that Big Co op, Inc. and EZ2Win.Biz had
5 operated at a loss in each year of its existence and had a continuing loss of over 4
6 million dollars by the end of 2006.
- 7 5. That almost all of the income for the company was generated by the sale of licenses
8 and fees charged to participants in the multilevel marketing scheme.
- 9 6. That income from Big Co op, Inc.'s "core business" of making commissions from the
10 sale of goods and services from third parties through the Big Co op internet shopping
11 network amounted to less than 1% of the company's income.
- 12 7. That the certified public accountant who prepared the financial statements for Big
13 Co op, Inc. for the years 2003 2006 had included a notice with the statements for
14 each of those years that Big Co op, Inc. had not been able to market its products at
15 amounts sufficient to recover its service and administrative costs and had suffered
16 consecutive losses for 5 years. The accountant's notice concluded "because of
17 uncertainties surrounding the ability of the company to continue its operations and
18 to satisfy its creditors on a timely basis, there is doubt about the company's ability
19 to continue as a going concern."

20 INVESTIGATION AIROSA

21 On May 29, 2007, I interviewed Joy Paguiso Airoso who told me the following:

- 22 1. In response to an investment tip from a neighbor she and her mother contacted
23 Patrick Ryan, President of EZ2Win.Biz. Ryan told them that Big Co op, Inc. was a
24 great investment opportunity that would be going public soon. The stock would be
25 worth \$50.00 per share when the company goes public.
- 26 2. Ryan told her that Big Co op, Inc. was an Internet shopping business that had
27 discount agreements with many big retail companies. like Sears, J.C. Penny,
28 Nordstrom's, and Target stores.

062 707 0.2

3. Ryan and others compared Big Co op. Inc.. with Google.
4. Based on this information her mother, on October 24, 2006. wrote a personal check (number 643) in the amount of \$25,000.00 made payable to EZ2Win.Biz as an investment in Big Co op. Inc.
5. Her mother and she didn't like the way Big Co op, Inc. handled their paperwork. For instance, it took the company until December 18, 2006, to get their stock certificate (for 28,000 shares) to them. They requested their money back soon after they invested.
6. After many telephone calls and e mail messages, on December 20, 2006. they got their money back in the form of a check (\$25,000) from another investor, not the company.

ALGREEN

On May 29, 2007, I interviewed Mrs. Ann Algreen who told me the following:

1. Her deceased husband made the investment in Big Co op, Inc. She attended some meetings with him and was involved in some conversations with Patrick Ryan who got him involved with the investment.
2. Her husband met Ryan at the country club where they all golfed. Ryan latched onto her husband who treated him like a son.
3. Ryan told them Big Co op was going public. As a result of Ryan's representations her husband invested \$104,000.00 in Big Co op, Inc.
4. At some point her husband and she started to have doubts about Big Co op, Inc. Ryan kept putting them off when they asked him about the company going public.
5. Ryan kept giving her husband and her excuses for the company not going public. One excuse he gave was that the company was meeting with overseas investors. Ryan also talked about the company doing something in India.
6. When her husband knew he was dying, he asked Ryan for their money back. Ryan told him he would have to check with his father, James Sweeney.

///

06270702

- 1 7. Before he died, her husband had a meeting with James Sweeney at Sweeney's office
2 In downtown Riverside. Their investment advisor accompanied her husband to this
3 meeting. Sweeney refused to give her husband their money back.

4 CICHY

5 On June 6, 2007, I interviewed Mr. Ron Cichy who told me the following:

- 6
7 1. He met Patrick Ryan at a bar in downtown Riverside (just down the street from
8 the business office). Ryan told him he had a great investment opportunity with
9 his Internet shopping company.
10 2. He befriended Ryan and they joined the Canyon Crest Country Club together.
11 3. He made several investments with Big Co op, Inc. beginning in November 2001
12 when he invested \$35,000.00 with the company. Ryan told him the stock was
13 worth \$1.00 per share, but would increase in value when the company goes
14 public. He invested a total of \$70,000.00 with the company.
15 4. In addition to investments in the company, he gave Ryan numerous personal loans
16 totaling in excess of \$50,000. He also paid many of Ryan's bills.
17 5. Ryan has since repaid most of the \$50,000.00 of personal loans, with company
18 checks [Ryan Enterprises (drawn on a Wells Fargo Bank account) and Big Co op,
19 Inc. (drawn on an Inland Empire National Bank account)].
20 6. Ryan told him the company was making money and was in the black. In fact,
21 Ryan told him that the company was making \$1 million per month.
22 7. Ryan told him "the auditors" were ready to go into the company and do an audit
23 so that the company would be closer to going public.
24 8. Ryan also mentioned a reverse merger being in the works in order to take the
25 company public.
26 9. He found out that the company was engaged in the sale of illegal securities. Ryan
27 told him 2 months ago (April 2007) that the company has spent \$500,000.00 in
28 legal fees to make the company legal.

///

06270702

- 1 10. Ryan gave him numerous reasons for the company not going public. One reason
- 2 was that a group of Norwegians were going to invest millions of dollars in Big Co
- 3 op. Inc.
- 4 11. The company would give away expensive gifts as inducements at sales meetings
- 5 for the multi level marketing program ran by Big Co op, Inc.

6 **DAKOTA**

7 On June 15, 2007, I interviewed Mr. John Dakota who told me the following:

- 8 1. He invested \$20,000.00 in Big Co op, Inc. after being told by Patrick Sweeney
- 9 (a/k/a Patrick Ryan) that it was a great opportunity.
- 10 2. Big Co op, Inc. would be going public within 90 days from his investment date or
- 11 he would get his money back.
- 12 3. After 90 days the company still had not gone public.
- 13 4. He asked Ryan why the company hadn't gone public and he was told it would be
- 14 another 90 days.
- 15 5. When the second 90 days passed and the company hadn't gone public, he asked
- 16 Ryan for his money back.
- 17 6. Ryan told him he would have to submit a letter to the company in order for the
- 18 legal channels to take place.
- 19 7. When he didn't get a response to his first letter, he telephoned Ryan and told him
- 20 he would go to the California Department of Corporations and to the News Media
- 21 if he didn't get his money back.
- 22 8. Ryan told him he would get his money back, but it would take approximately 4
- 23 months at \$5,000.00 per month to do so. He got his money back within 4 months.
- 24 9. As he recalls the checks paying back his investment were drawn on an account at
- 25 Wells Fargo Bank.
- 26 10. When he invested with the company, Ryan was the President of EZ2Win.Biz,
- 27 which is the marketing side of Big Co op, Inc. James Sweeney was the CEO of
- 28 Big Co op, Inc.

06270702

WALLING

On June 20, 2007, I contacted Mr. Russell Walling, Owner/Building Manager, 3666 University Avenue, Suite 405, Riverside, California. He told me the following:

1. He has known James Sweeney doing business as Big Co op, Inc. for 8 or 9 years, when he moved into the building.
2. Sweeney and his adopted son, Patrick Ryan, seemed to alternate as president of the company.
3. He has tried to help Sweeney with his business over the years and consequently Sweeney owes him \$229,000.00 in back rent over a 3 or 4 year period.
4. On or about June 6, 2007, Sweeney moved out of the building without paying his back rent.
5. Mr. Walling took possession of 9 Dell desktop computers belonging to Sweeney and his business; Sweeney and his business associates had abandoned the computers. After taking the nine (9) Dell desktop computers from the Big Co-op offices, Mr. Walling had the entrance doors to the 3rd floor re-keyed.
6. Sweeney took the computer that was in his office, Ryan took the computer that was in his office; and Ryan's ex wife, Kelli Ryan, who was also the company's chief financial officer/bookkeeper, took the computer that was in her office.
7. He has the 9 Dell computers on tables in a storage room in the basement of the building.
8. He knows that Sweeney and Ryan did their business banking at Wells Fargo Bank, which is down the street on University; and the Inland Empire National Bank, which is on the mall on Main Street.

OBSERVATIONS ON THE THIRD (3RD) FLOOR

On June 20, 2007, Mr. Walling gave me a tour of the third (3rd) floor of his building. This is the floor space that was occupied by Sweeney and his associates doing business as Big Co-op, Inc. and EZ2Win.Biz. While touring the third (3rd) floor of the building, I observed the following:

///

06270702

- 1 1. Walling unlocked the front entrance door to the suite of offices on the third (3rd)
- 2 floor with a key that was on a large ring with other keys.
- 3 2. I observed a large open area that ran from one end of the third floor to the other
- 4 end. This open area had individual offices off of it. I estimated that there are 8 to
- 5 10 individual offices within the office suite. Some offices are larger than others.
- 6 Mr. Walling told me that Sweeney and Ryan had the larger offices.
- 7 3. Inside most of the individual offices, I saw trash receptacles filled with what
- 8 appeared to be computer instruction manuals, Big Co-op/EZ2Win.Biz business
- 9 instruction manuals and other documents.
- 10 4. I observed the offices to be virtually empty except for the trash receptacles and
- 11 some office furniture.

12 BANK LOCATIONS TO BE SEARCHED

13 With regard to the Wells Fargo Bank accounts at 3750 University Avenue, Riverside,
14 California and the accounts at Inland Empire National Bank at 3737 Main Street, Suite 104,
15 Riverside, California, based on the below information and my experience, I believe there is probable
16 cause to believe that there are Ryan Enterprises, Big Co op, Inc. and EZ2Win.Biz, Inc., as well as
17 Sweeney and Ryan financial records, which are on the premises and are evidence of the crimes
18 described below.

19 BASEMENT STOREROOM LOCATION

20 With respect to the nine (9) Dell desktop computers currently being stored in the basement
21 storeroom at the Walling Building, 3666 University Avenue, Riverside, California, based on the
22 below information and my experience I believe there is probable cause to believe that there are
23 business and financial records related to Ryan Enterprises, Big Co op, Inc. and EZ2Win.Biz, Inc.,
24 which are on the premises and are evidence of the crimes described below.

25 THIRD FLOOR WALLING BUILDING LOCATION

26 With respect to the third floor of the Walling Building, 3666 University Avenue, Riverside,
27 CA 92501, based on the above information and my experience, I believe there is probable cause to
28 believe that there are computer instruction manuals and Big Co-op, Inc./EZ2Win.Biz business

06270702

1 manuals and other documents in trash receptacles in the individual offices within the suite of offices
2 on the third (3rd) floor, which are on the premises and are evidence of the crimes described below.

3 **PERSONAL RESIDENCES**

4 With respect to the personal residences of Patrick Michael Ryan, 1048 Peter Christian Circle,
5 Corona, California 92881; and the residence of Kelli Ann Ryan, the company's chief financial
6 officer/bookkeeper, 29449 Tours Street, Lake Elsinore, California, based on the information
7 described herein and my experience I believe there is probable cause to believe that there are Ryan
8 Enterprises, Big Co op, Inc. and EZ2Win.Biz, Inc., business records and financial information,
9 which are on the premises and is evidence of the crimes described below.

10 Based on the information contained herein, my experience and the experience of other agents and
11 investigators with whom I have worked, I believe there is probable cause to believe that the bank
12 records and the electronic records requested in this affidavit and stored in the nine (9) Dell desktop
13 computers kept in the basement storage room of the Walling Building and the two (2) computers
14 kept in the separate, personal residences of Patrick Ryan and his ex-wife, Kelli Ann Ryan, as well
15 as the instruction and business manuals contained in trash receptacles on the third (3rd) floor of the
16 Walling Building contain evidence of the on going securities fraud and theft perpetrated on the
17 public by James Albert Sweeney II and Patrick Michael Ryan doing business as Ryan Enterprises,
18 Big Co op, Inc. and EZ2Win.Biz, Inc., as described below:

19 **APPLICABLE CRIMINAL STATUTES**

20 Section 25401 of the California Corporate Securities law states that it is unlawful for any
21 person to offer or sell a security in this state or buy or offer to buy a security in this state by means
22 of any written or oral communication which also includes an untrue statement of material fact or
23 omits to state a material fact necessary in order to make the statements made in light of the
24 circumstances under which they were made, not misleading.

25 Section 25110 of the California Corporation Securities Law states that it is unlawful for any
26 person to offer or sell in this state any security in an issuer transaction unless such sale has
27 been qualified under section 25111, 25112 or 25113 or unless such security or transaction is
28 exempted or not subject to qualification.

06270702

1 Section 25540(a) of the California Corporate Securities Law states any person who willfully
2 violates any provision of the Corporate securities Law of 1968, or who willfully violates any rule
3 or order under said division, shall upon conviction be fined not more than one million dollars
4 (\$1,000,000) , or imprisoned in the state prison, or in county jail for not more than one year, or be
5 punished by both fine and imprisonment.

6 Section 25540(b) of the California Corporate Securities law sates any person who willfully
7 violates section 25400, 25401 or 25402, or who willfully violates any rule or order under the
8 Corporate Securities Law of 1968, adopted pursuant to those provisions, shall upon conviction be
9 fined not more than ten million dollars (\$10,000,000), or imprisoned in the state prison for two (2),
10 three (3), or five (5) years, or be punished by both fine and imprisonment.

11 Section 327 of the California Penal Code states that it is unlawful for any person to contrive,
12 prepare, set up, propose, or operate any endless chain an "endless chain" means any scheme for the
13 disposal or distribution of property whereby a participant pays a valuable consideration for the
14 chance to receive compensation for introducing one or more additional persons into the participation
15 in the scheme or for the chance to receive compensation when a person introduced by the participant
16 introduces a new participant. This crime is punishable by Imprisonment in the county jail not
17 exceeding one year or in the state prison for 16 months, two or three years.

18 Section 487 of the California Penal code states that Grand Theft is committed in any of the
19 following cases: (a) when the money, labor or real or personal property taken is of a value exceeding
20 four hundred dollars (\$400).

21 **WELLS FARGO AND INLAND EMPIRE NATIONAL BANKS**

22 On June 20, 2007, I went to the Wells Fargo Bank, which is down the street from the
23 Walling Building (3666 University Avenue) and observed that the address is 3750 University
24 Avenue (the Riverside Main Office), Riverside, California 92501.

25 On June 20, 2007, I went to the Inland Empire National Bank, which is on the mall on
26 Main Street as described by Mr. Walling and learned the following:

27 1. The address is 3737 Main Street, Suite 104, Riverside, California 92501.

28 ///

06270702

2. Alice Henderson is the Operations Manager at this bank. She told me that:

- a. She knows the business name Big Co op, Inc.
- b. Account number: 001515756 is maintained at her branch.
- c. Legal documents should be served on the main office at 3727 Arlington Avenue, Riverside, CA 92706.

During the investigation I reviewed the checks given me by investors Airosa/Paguio and Cichy and learned the following:

1. The check Paguio used to pay Big Co op, Inc (EZ2Win.Biz) showed the following:
 - a. The check number is 643 and is dated 10/24/2006; it is made payable to EZ2Win.Biz in the amount of \$25,000.00.
 - b. The back of the check shows that it was deposited to an account titled EZ2Win.BIZ; the number is 6655853429 (I have seen this same series of numbers on a Wells Fargo Bank check written to Mr. Cichy).
2. One of the checks given me by Mr. Cichy was drawn on a Well Fargo Bank account (number: 6655851878). It is check number 1077 and is dated 1/10/2006. The check is in the amount of \$1,000.00. The memo section of the check reads: "loan pay back to him." The account name is Ryan Enterprises, 3666 University Ave. FL 3, Riverside, CA 92501-3346.
3. Another check given me by Mr. Cichy shows the following:
 - a. The check number is 3209 drawn on Inland Empire National Bank, Riverside, CA 92501. The check is dated 6/8/2004.
 - b. The account name is Big Co op, Inc., 3666 University Ave. 3RD Floor, Riverside, CA 92501.
 - c. The account number is 001515756.

PERSONAL RESIDENCE PATRICK RYAN (A/K/A PATRICK SWEENEY)

When interviewed June 20, 2007, Mr. Russell Walling reported that Patrick Ryan had taken his desktop computer from his office on June 6 8, 2007. During the investigation I learned that

06270702

1 Patrick Ryan lives at 1048 Peter Christian Circle, Corona, California 92881. On June 25, 2007, I
2 went to the address 1048 Peter Christian Circle, Corona, California 92881 and observed the
3 following:

- 4 1. A dark blue Mercedes Benz bearing California license plate number "5YGT009"
5 was parked in the driveway. Another dark colored Mercedes Benz bearing no
6 license plates was parked on the street in front of the house.
- 7 2. A subsequent check with the California Department of Motor Vehicles revealed
8 that plate number "5YGT009" is registered to Patrick Ryan and/or Kelli Ryan,
9 1048 Peter Christian Circle, Corona, California.

10 PERSONAL RESIDENCE KELLI RYAN

11 When he was interviewed on June 20, 2007, Mr. Walling told me that Kelli Ryan was the
12 chief financial officer/bookkeeper for the Big Co op, Inc. and EZ2Win.Biz business. He said he
13 knows that she took the desktop computer that she used at the business. During the investigation,
14 I learned that Kelli Ryan lives at 29449 Tours Street, Lake Elsinore, California. On June 25, 2007,
15 I went to the address 29449 Tours Street, Lake Elsinore, California, and observed the following:

- 16 1. A new looking dark blue Mercedes Benz bearing personalized California license
17 plates "SXYCFO" was parked in the driveway. There were two (2) other vehicles
18 parked in the driveway also. One was a dark colored Cadillac Escalade with no
19 plates; the other was a dark colored SUV bearing personalized California license
20 plates "WUCARDZ."
- 21 2. A subsequent check with the California Department of Motor Vehicles revealed
22 that plate number "5YGT009" is registered to Kelli Ann Ryan, 29449 Tours
23 Street, Lake Elsinore, California.

24 SEIZURE OF DIGITAL EVIDENCE

25 With respect to the nine (9) Dell computers currently being stored in the basement storeroom
26 of the Walling Building at 3666 University Avenue, Riverside, California 92501; and the three (3)
27 desk top computers taken from the business location by James Albert Sweeney, Patrick Michael
28 Ryan, and Patrick Ryan's ex wife, Kelli Ann Ryan and believed to be kept at their personal

06270702

1 residences, I have consulted with Robert Werbick, whom I have known and worked with for over
2 15 years. Robert Werbick has been employed as a Postal Inspector with the United States Postal
3 Inspection Service, Los Angeles Division since November 1991. Beginning in December 2001,
4 Postal Inspector Werbick has been assigned to the Forensic Laboratory Services Division, Dulles,
5 Virginia as Program Manager, Digital Evidence Unit domiciled in Anaheim, CA, where his duties
6 have included the investigation of criminal offenses including high technology crime, account
7 fraud, check fraud, and identity theft and the forensic examination of computers. Postal Inspector
8 Werbick possesses a Bachelor of Science degree in electrical engineering from California
9 Polytechnic University, Pomona, California. He has attended numerous specialized training courses
10 in forensic science, including training in Encase forensic science.

11 Based on my training, experience and my conversations with Postal Inspector Werbick, I am
12 aware of the following: (1) that individuals engaged in securities fraud and grand theft often use
13 computers as tools of their crime, to store clients' personal and account information, to create
14 company records, correspondence to clients/customers, and company update information and to
15 store company and personal financial transaction records; (2) that suspects use computers to obtain
16 goods, services, and/or other personal and company assets; (3) that computer users will commonly
17 keep computers and computer systems in their homes and places of employment; (4) that computer
18 users frequently back up copies of software to guard against loss if their computer malfunctions;
19 they keep those backup copies at their residence and/or place of employment; and (5) that software
20 and digital data is portable and is often transported to and from residences in automobiles and is
21 occasionally hidden in automobiles.

22 In addition, Postal Inspector Werbick advised me why all computers and computer
23 equipment must be removed from search warrant sites and searched under controlled circumstances.
24 Because of the ways in which computer technologies store or process data, files relating to criminal
25 investigations are often stored with unrelated records. In order to determine which records may be
26 seized pursuant to a search warrant, it is necessary to use appropriate forensic software to open and

27 ///

28 ///

06270702

1 view the contents of all files. Postal Inspector Werbick further advised me that the file name in the
2 folder/directory is not a reliable indicator of the true nature of its contents, especially where there
3 may be a desire on the user's part to conceal certain records.

4 Postal Inspector Werbick has also been trained in methods to recover hidden, deleted, and
5 erased files. Based on his experience and training, he advises me that digital files reside, in whole
6 or in part, on a computer's hard drive or other external electronic storage media until they are
7 overwritten. Under many operating systems software (including Microsoft Windows 95 or higher),
8 it is frequently possible to reconstruct deleted or erased files, as well as the fact of the deletion and
9 the time and date of the deletion. Such facts can be evidence of an attempt to destroy, hide or
10 fabricate evidence, and may be evidence of consciousness of guilt. According to Postal Inspector
11 Werbick, computer users may also conceal data through a number of methods, including the use of
12 misleading filenames and extensions. For example, files with the extension ".jpg" are digital image
13 files. However, a computer user could change a ".jpg" file extension to ".txt" or ".dll," in order to
14 create an appearance that a digital image is actually a text or system file. It is often difficult for an
15 investigator to notice such anomalies without conducting a properly controlled forensic examination
16 at a location away from the search site.

17 Postal Inspector Werbick advised me that conducting a search of a computer system's files,
18 documenting the search, and making evidentiary and discovery copies is a lengthy and time
19 consuming process, particularly with the increased data storage capacity of newer computers. He
20 said it is also necessary to determine that no security devices are in place, both hardware and
21 software, which could cause the destruction of evidence during the search. He said in some cases
22 it is impossible even to conduct the search without expert technical assistance, especially if the
23 data is stored on a network server and/or Unix operating system. He said expert technical assistance
24 may also be required if the computer system and files have been protected using an encryption
25 method. Since computer evidence is extremely vulnerable to tampering or destruction through error,
26 electrical outages, and other causes, the removal of the system from the premises will greatly assist
27 in retrieving the records authorized to be seized, while avoiding destruction or deliberate alteration
28 of the records. He said it would be very difficult to search the computer system's files on the

06270702

1 premises during the execution of a search warrant. Instead, a search could take several weeks or
2 months, depending on the technical difficulties encountered. He told me that in almost every
3 instance the suspect's computer(s) and removable electronically stored media should be removed
4 from the crime scene and their contents be examined in a controlled environment to preserve the
5 evidentiary integrity of the data.

6 Postal Inspector Werbick advised me that any use of a subject's computer to examine files
7 should be avoided, since it could be rigged to destroy or alter data. He also told me that it is
8 impossible to ensure that any equipment brought by law enforcement personnel to a search site could
9 be used to adequately examine storage media present at the location, since the type and quantity of
10 storage media is usually not known prior to conducting a search. In addition, it is impossible to
11 predict which application programs, drivers, and other software (out of hundreds available on the
12 market) have been used by the subject to create files stored on the computer media.

13 For this reason, Postal Inspector Werbick advised me that all software associated with any
14 seized computer must also be seized since it would be impossible, without examination, to determine
15 if it is standard commercially available software. He said in many instances it is necessary to
16 examine the software applications used to create files in order to read the files. Additionally,
17 without examination, it is impossible to determine if a disk, purporting to contain a standard
18 commercially available software program, is also being used to store data or information relevant
19 to the ongoing investigation.

20 I was also advised by Postal Inspector Werbick that system documentation, instruction
21 manuals, and software manuals relating to the computer system also need to be seized in order to
22 properly operate that specific system, and to accurately obtain and copy the records and files
23 authorized to be seized. This documentation may also further assist in establishing the ownership
24 and/or the operator of the computer system being seized. He also told me that computer users
25 frequently employ passwords to protect their data files and records. He said that in many instances
26 the computer user will often write passwords in their system manuals, notebooks, on post it notes,
27 etc., and it is therefore necessary to seize all written material that is in close proximity of a computer
28 system being seized.

n6270702

1 premises during the execution of a search warrant. Instead, a search could take several weeks or
2 months, depending on the technical difficulties encountered. He told me that in almost every
3 instance the suspect's computer(s) and removable electronically stored media should be removed
4 from the crime scene and their contents be examined in a controlled environment to preserve the
5 evidentiary integrity of the data.

6 Postal Inspector Werbick advised me that any use of a subject's computer to examine files
7 should be avoided, since it could be rigged to destroy or alter data. He also told me that it is
8 impossible to ensure that any equipment brought by law enforcement personnel to a search site could
9 be used to adequately examine storage media present at the location, since the type and quantity of
10 storage media is usually not known prior to conducting a search. In addition, it is impossible to
11 predict which application programs, drivers, and other software (out of hundreds available on the
12 market) have been used by the subject to create files stored on the computer media.

13 For this reason, Postal Inspector Werbick advised me that all software associated with any
14 seized computer must also be seized since it would be impossible, without examination, to determine
15 if it is standard commercially available software. He said in many instances it is necessary to
16 examine the software applications used to create files in order to read the files. Additionally,
17 without examination, it is impossible to determine if a disk, purporting to contain a standard
18 commercially available software program, is also being used to store data or information relevant
19 to the ongoing investigation.

20 I was also advised by Postal Inspector Werbick that system documentation, instruction
21 manuals, and software manuals relating to the computer system also need to be seized in order to
22 properly operate that specific system, and to accurately obtain and copy the records and files
23 authorized to be seized. This documentation may also further assist in establishing the ownership
24 and/or the operator of the computer system being seized. He also told me that computer users
25 frequently employ passwords to protect their data files and records. He said that in many instances
26 the computer user will often write passwords in their system manuals, notebooks, on post it notes,
27 etc., and it is therefore necessary to seize all written material that is in close proximity of a computer
28 system being seized.

06270702

1 Therefore, I request that investigating officers be authorized, at their discretion, to seize all
2 "computer systems," "computer program or software," and "supporting documentation" as defined
3 by Penal Code section 502, subdivision (b), including any peripherals, and any supporting hardware,
4 software, and to conduct an off site search of the seized items for the evidence described in this
5 affidavit. I further request that investigating officers, and those agents acting under the direction of
6 the investigating officers, be authorized to access all computer data to determine if the data contains
7 "property," "records," and "information," and that, if necessary, investigating officers be authorized
8 to employ the use of outside experts, acting under the direction of the investigating officers, to
9 access and preserve computer data. I request authorization for investigating officers to seized any
10 digital evidence found during the execution of this search warrant, to transported such evidence from
11 the search location, and to conduct a search and analysis at a location designated by investigating
12 officers. With respect to any above described computer found during a search executed within ten
13 days of the issuance of this warrant, I request authorization for officers or their agents to seize,
14 transport, and analyze such computers, and that such a search may continue beyond ten (10) days
15 after the issuance of the search warrant.

16 I also request permission to videotape and/or photograph the execution of this search
17 warrant. I expect to examine computer(s) at the scene of the search. Those computers may be
18 operating when I arrive at the premises. The images on the screens of the computers are transient,
19 meaning that they disappear when the computer is turned off. I need to be able to videotape and/or
20 photograph any such images because they may be evidence (e.g., incriminating documents being
21 written by the user when the search warrant is executed). The videotape or photographs may be
22 useful in documenting what was done to the computers. Photography of the location and persons
23 present at the scene is also often helpful in showing possession of the premises and evidence of
24 association of the parties.

25 CONCLUSION

26 Based on the information contained herein, my experience and the experience of other agents
27 and investigators with whom I have worked, I believe there is probable cause to support the issuance
28 of search warrants as set forth in Penal Code Section 1524 to search for any accounts listed in
Attachment "A" and to provide all information from those accounts to me. I believe there is

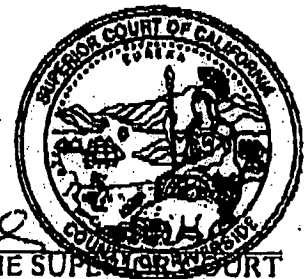
06270702

1 probable cause to support the issuance of a search warrant as set forth in Penal Code Section 1524
2 to search for and seize the nine (9) Dell computers currently being stored by Mr. Russell Walling
3 in the basement of his office building as well as the desk top computers taken from the business
4 location and believed to be kept at the personal residences of Patrick Michael Ryan and Patrick
5 Ryan's ex wife, Kelli Ann Ryan. Additionally, I believe there is probable cause to support the
6 issuance of a search warrant as set forth in Penal Code Section 1524 to search for and seize financial
7 and business records as well as computer and business manuals currently kept in trash receptacles
8 in offices on the third (3rd) floor of the Walling Building. These documents and records will assist
9 in determining if James Albert Sweeney II and Patrick Michael Ryan doing business as Ryan
10 Enterprises, Big Co op, Inc. and EZ2Win.Biz, Inc., have committed grand theft and fraud.
11 Deputy Attorney General Patricia Fusco has reviewed this document.

12 Given under my hand and dated this 27 day of June 2007.

13
14 Aaron L. Ward
15 Aaron L. Ward 7/19/2007

16 Subscribed and sworn to before
17 me this 27 day of June 2007,
18 at 9:30 A.M./P.M.



18 Patricia Fusco
19 JUDGE OF THE SUPERIOR COURT
20 CLERK
21 Patricia Fusco
22 DEPUTY CLERK
23
24
25
26
27
28

Patricia Fusco

ATTACHMENT D

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

0718070

RECEIVED
SUPERIOR COURT OF CALIF.
COUNTY OF RIVERSIDE

Supplement

1
2007 JUL 18 AM 9:41

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT
EXPERIENCE AND TRAINING OF AFFIANT

BY: 3 I, Aaron L. Ward, am an Investigator with the California Department of Justice (DOJ),
4 Special Crimes Unit, Office of the Attorney General. I have been employed as an Investigator with
5 the Department of Justice since April 2, 2001. Prior to my employment as an investigator with the
6 California Department of Justice, I was a United States Postal Inspector assigned to the Southern
7 California Division of the United States Postal Inspection Service. I retired from the position of
8 Postal Inspector on March 30, 2001, and took my current position. I was a Postal Inspector for
9 twenty years. For the last ten years of my Inspection Service career, my responsibilities included
10 investigating crimes involving mail fraud and supervising the activities of five other Postal
11 Inspectors. I have extensive experience investigating crimes involving financial transactions,
12 investment fraud schemes (including Ponzi schemes), and money laundering.

13 I completed an eleven-week training course for Postal Inspectors at the United States Postal
14 Inspection Service (USPIS) Academy at Potomac, MD. I have attended both basic and complex
15 fraud training courses at the USPIS Academy in Potomac, MD. Additionally, I have received money
16 laundering and asset forfeiture training at the USPIS Academy in Potomac, MD. I have received
17 bankruptcy fraud training at the United States Attorney's Office (USAO), Central District of
18 California (CDC), Los Angeles, CA.

19 I have provided training on workers' compensation fraud investigations to other postal
20 inspectors. I have testified as an expert witness for the USAO, CDC, Los Angeles, CA., related to
21 telemarketing fraud investigations.

22 I have been a participant in the United States Attorney's Office, Southern California,
23 Investment Fraud Task Force, formed to pool resources and experiences in the investigation of
24 violations and abuses in the area of "boiler-room" schemes. I have also been a member of the
25 County of Orange Boiler-room Apprehension (COBRA) Task Force, which was comprised of
26 various federal and state agencies that investigated alleged telemarketing "boiler-room" fraud.

27 ///
28 ///

ATTACHMENT D

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

0718070

RECEIVED
SUPERIOR COURT OF CALIF.
COUNTY OF RIVERSIDE

Supplement
AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

2007 JUL 18 AM 9:41

EXPERIENCE AND TRAINING OF AFFIANT

BY: 3 J. Aaron L. Ward, am an Investigator with the California Department of Justice (DOJ),
4 Special Crimes Unit, Office of the Attorney General. I have been employed as an Investigator with
5 the Department of Justice since April 2, 2001. Prior to my employment as an investigator with the
6 California Department of Justice, I was a United States Postal Inspector assigned to the Southern
7 California Division of the United States Postal Inspection Service. I retired from the position of
8 Postal Inspector on March 30, 2001, and took my current position. I was a Postal Inspector for
9 twenty years. For the last ten years of my Inspection Service career, my responsibilities included
10 investigating crimes involving mail fraud and supervising the activities of five other Postal
11 Inspectors. I have extensive experience investigating crimes involving financial transactions,
12 investment fraud schemes (including Ponzi schemes), and money laundering.

13 I completed an eleven-week training course for Postal Inspectors at the United States Postal
14 Inspection Service (USPIS) Academy at Potomac, MD. I have attended both basic and complex
15 fraud training courses at the USPIS Academy in Potomac, MD. Additionally, I have received money
16 laundering and asset forfeiture training at the USPIS Academy in Potomac, MD. I have received
17 bankruptcy fraud training at the United States Attorney's Office (USAO), Central District of
18 California (CDC), Los Angeles, CA.

19 I have provided training on workers' compensation fraud investigations to other postal
20 inspectors. I have testified as an expert witness for the USAO, CDC, Los Angeles, CA., related to
21 telemarketing fraud investigations.

22 I have been a participant in the United States Attorney's Office, Southern California,
23 Investment Fraud Task Force, formed to pool resources and experiences in the investigation of
24 violations and abuses in the area of "boiler-room" schemes. I have also been a member of the
25 County of Orange Boiler-room Apprehension (COBRA) Task Force, which was comprised of
26 various federal and state agencies that investigated alleged telemarketing "boiler-room" fraud.

27 ///

28 ///

07180701

1 During my career as a postal inspector, I have been the affiant on approximately 60 search warrant
2 affidavits, requesting to search and seize electronic files contained in computer equipment, bank
3 accounts, brokerage accounts, and records from business and residential premises. In virtually every
4 instance in which a search warrant was issued, I found evidence of the crime alleged. I am familiar
5 with the United States Code and the California Penal Code relating to financial crimes, conspiracy,
6 and the rules of evidence.

7 INTRODUCTION

8 This case was referred to the Department of Justice, Office of the Attorney General, in April
9 2007, after complaints by investors about the individuals and companies discussed below. The
10 Department of Corporations (DOC) enforcement attorney, Kirk Wallace, referred the case for the
11 reason that it was believed the below-described individuals were operating an endless-chain
12 marketing scheme and had defrauded investors of approximately \$5 Million in unregistered stock. In
13 addition to selling memberships, in violation of the California Corporate Securities laws, as well as
14 the California Penal Code. The DOC has issued two Desist and Refrain Orders against James Albert
15 Sweeney, Big Co-Op, Inc. and EZ2Win.Biz and others. After the most recent Desist and Refrain
16 Order was served, Attorney Wallace informed us that Mr. Sweeney had started a new company to
17 continue Big Co-Op's Business. The name of that business is Together4Good, a Nevada
18 Corporation.

19 This supplemental affidavit is being submitted in support of applications for search warrants
20 on the residence of James Albert Sweeney, CEO, Big Co-op, Inc. and EZ2Win.Biz, 4555 Mission
21 Inn Avenue, Riverside, California and two (2) storage units maintained by Sweeney at A-American
22 Self-Storage at 2431 Rubidoux Avenue, Riverside, California

23 On Wednesday, June 27, 2007, Superior Court Judge J. A. Edwards authorized six search
24 warrants (No: 06270702) relating to this matter. The Affidavit submitted in support of those six (6)
25 search warrants is incorporated herein by reference and is attached to this supplemental affidavit as
26 exhibit 1. One of the six search warrants was for the residence of Kelli Ann Ryan, CFO, Big Co-op,
27 Inc. and EZ2Win.biz. I was a member of the task force that searched Ms. Ryan's residence. During
28 the search of Ms. Ryan's residence, she told me the following:

07180701

- a. She resigned her position at Big Co-op, Inc and EZ2Win.Biz in May 2007.
- b. In early June 2007, James Sweeney moved his business out of the offices at 3666 University Avenue, 3rd Floor, Riverside, CA.
- c. Sweeney took desktop computer that she used to use in her work for Big Co-Op, Inc/EZ2Win.Biz, wiped the computer's hard drive, and then gave the computer to her.
- d. The computer Sweeney gave to her still has the company's (Big Co-Op, Inc/EZ2Win.Biz) financial files on it in the form of QuickBooks files.
- e. She has spoken to Richard Hickey who used to work with her at Big Co-Op, Inc/EZ2Win.Biz and he told her he packed up a number of boxes with business records and took them to Sweeney's personal residence and placed many of the boxes in Sweeney's garage. When the garage got too full he took some boxes to the storage units.
- f. Sweeney lives at 4555 Mission Inn Avenue, Riverside, California.
- g. Sweeney had 3 storage units at A-American Self-Storage, Riverside, California. She believes he now has two (2) units there.

On Monday, July 2, 2007, I went to the address 4555 Mission Inn Avenue, Riverside, California, and observed the following:

- h. The residence is a 2-story single-family residence on the north side of Mission Inn Avenue. Redwood Drive is to the east. It is dark tan in color and trimmed in a maroon and blue. The residence has an orange colored, ceramic tile roof.
- i. There is a balcony on the second floor of the residence.
- j. Entrance to the residence is through a single glass door framed in wood (colored maroon). The entrance door is in the center of the residence.
- k. There are 2 sets of stairs leading from the street to the entrance doors. There are 2 statues of lions (white in color) on either side of the steps closest to the entrance door.

///

1 On Monday, July 2, 2007, I spoke with Postal Inspector Dave Zemke who told me that he
2 had checked on the address, 4555 Mission Inn Avenue, with the Riverside Post Office and learned
3 that James A. Sweeney receives mail at the address.

4 On Thursday, July 12, 2007, I went to the A-American Self-Storage at 2431 Rubidoux
5 Avenue, Riverside, California and learned the following:

- 6 a. The above location is a commercial structure located in the city and
7 the county of Riverside. It has a gray exterior, trimmed in dark blue.
- 8 b. The property is clearly marked by signage at the intersection of
9 Rubidoux and 24th Streets that reads: A-American Self Storage. The
10 signage is on a white back ground with blue letters and three wavy
11 horizontal lines (denoting the American Flag) after the first "A." The
12 signage can be seen from Rubidoux Avenue and there is a sign on 24th
13 Street.
14
- 15 c. Entrance to the self-storage unit is off of 24th Street. Unit numbers
16 142 and 162 are on the east side of the main driveway leading from
17 24th Street.
18
- 19 d. Unit number 142 is 10' by 18'. It is clearly marked by the numbers
20 142 that are white in color and are affixed to the wall on the storage
21 unit about ½ up the overhead door. There are red fire extinguishers
22 mounted on the exterior of the storage units walls. The fire
23 extinguishers are at every five storage units. Unit 142 is two (2) fire
24 extinguishers from the entrance gate. The overhead door is dark blue
25 in color.
26
- 27 e. Self-Storage unit 162 is 10' by 15'. It is located on the same side of
28

07180701

1 the driveway as unit 142. It is clearly marked by the numbers 162 that
2 are white in color and are affixed to the wall on the storage unit about
3 ½ up the overhead door. The overhead door is dark blue in color.

4 Unit 162 is near the fifth fire extinguisher.

5 f. James Sweeney doing business as Big Co-op, Inc. rents units 142 and
6 162.

7 g. Sweeney was in earlier that day to argue about being assessed a late
8 fee

9 of \$20.00 for being late paying for the rental of the storage units.

10 APPLICABLE CRIMINAL STATUTES

11 Section 25401 of the California Corporate Securities law states that it is unlawful for any
12 person to offer or sell a security in this state or buy or offer to buy a security in this state by means of
13 any written or oral communication which also includes an untrue statement of material fact or omits
14 to state a material fact necessary in order to make the statements made in light of the circumstances
15 under which they were made, not misleading.

16 Section 25110 of the California Corporation Securities Law states that it is unlawful for any
17 person to offer or sell in this state any security in an issuer transaction...unless such sale has been
18 qualified under section 25111, 25112 or 25113...or unless such security or transaction is exempted
19 or not subject to qualification...

20 Section 25540(a) of the California Corporate Securities Law states any person who willfully
21 violates any provision of the Corporate securities Law of 1968, or who willfully violates any rule or
22 order under said division, shall upon conviction be fined not more than one million dollars
23 (\$1,000,000), or imprisoned in the state prison, or in county jail for not more than one year, or be
24 punished by both fine and imprisonment.

25 Section 25540(b) of the California Corporate Securities law sates any person who willfully
26 violates section 25400, 25401 or 25402. or who willfully violates any rule or order under the
27 Corporate Securities Law of 1968, adopted pursuant to those provisions, shall upon conviction be
28

071 80701

1 fined not more than ten million dollars (\$10,000,000), or imprisoned in the state prison for two (2),
2 three (3), or five (5) years, or be punished by both fine and imprisonment. Section 327 of the
3 California Penal Code states that it is unlawful for any person to contrive, prepare, set up, propose,
4 or operate any endless chain...an "endless chain" means any scheme for the disposal or distribution
5 of property whereby a participant pays a valuable consideration for the chance to receive
6 compensation for introducing one or more additional persons into the participation in the scheme or
7 for the chance to receive compensation when a person introduced by the participant
8 introduces a new participant. This crime is punishable by imprisonment in the county jail not
9 exceeding one year or in the state prison for 16 months, two or three years.

10 Section 487 of the California Penal code states that Grand Theft is committed in any of the
11 following cases: (a) when the money, labor or real or personal property taken is of a value exceeding
12 four hundred dollars (\$400)...

13 CONCLUSION

14 With respect to the personal residence of James A. Sweeney I believe there is probable cause
15 to support the issuance of a search warrant to search the premises described in Attachment A,
16 location 1, as set forth in Penal Code Section 1524 to search for and seize financial and business
17 records in any form as described in Attachment B. Records in the form of electronic files stored on
18 computers will be treated as indicated in exhibit 1, pages 12 through 17. These documents and
19 records will assist in determining if James Albert Sweeney II and Patrick Michael Ryan doing
20 business as Ryan Enterprises, Big Co-op, Inc. and EZ2Win.Biz, Inc., have committed grand theft
21 and fraud.

22 With respect to the 2 storage units maintained by James A. Sweeney at A-American Self-
23 Storage, 2431 Rubidoux Avenue, Riverside, California, I believe there is probable cause to support
24 the issuance of search warrants as set forth in Penal Code Section 1524 to search the self-storage
25 units described in Attachment A, location 2 for and seize financial and business records in any form
26 described in Attachment B. Records in the form of electronic files stored on computers will be
27 treated as indicated in exhibit 1, pages 12 through 17. These documents and records will assist in
28 ///

1 ///
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

07180701

1 determining if James Albert Sweeney II and Patrick Michael Ryan doing business as Ryan
2 Enterprises, Big Co-op, Inc. and EZ2Win.Biz, Inc., have committed grand theft and fraud.

3 Deputy Attorney General Patricia Fusco has reviewed this document.

4 Given under my hand and dated this _____ day of July 2007.

5

6

7



Aaron L. Ward

8

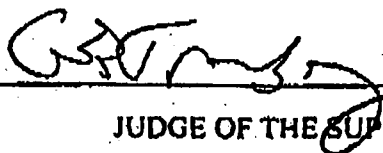
9 Subscribed and sworn to before

10 me this 15th day of July 2007,

11 at _____ A.M./P.M.

12

13



14

JUDGE OF THE SUPERIOR COURT

15

16

17

18

19

20

21

22

23

24

25

26

27

28